



Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

Declaración de seguridad
(low assurance)

Descarga de datos procedentes del Tacógrafo Digital
Versión: 1.6, 11/06/2009



DOCUMENTO:	DECLARACIÓN DE SEGURIDAD. DESCARGA DE DATOS DEL TACÓGRAFO DIGITAL
AUTOR:	FNMT-RCM
REVISION	FNMT-RCM
VERSIÓN:	1.6
FECHA:	11/06/2009

Índice

1	<i>Identificación de la Declaración de Seguridad</i>	9
1.1	Identificación del Objetivo de la Evaluación	9
1.2	Resumen	9
1.3	Ajuste a la norma “Common Criteria”	9
2	<i>Descripción del producto a evaluar.</i>	11
3	<i>Objetivos de seguridad para el entorno</i>	13
3.1	Objetivos del entorno IT	13
4	<i>Requisitos de seguridad.</i>	14
4.1	Requisitos funcionales de seguridad	14
4.1.1	FDP_ETC.2 Export of user data with security attributes	14
4.1.2	FDP_ITC.2 Import of user data with security attributes	14
4.1.3	FDP_IFC.1 Subset information flow control	15
4.1.4	FPT_TDC.1 Inter-TSF basic TSF data consistency	15
4.1.5	FDP_IFF.1 Simple security attributes	16
4.2	Requisitos de garantía de seguridad	17
4.3	Justificación de requisitos de seguridad	17
5	<i>Resumen de la especificación</i>	19

Índice de tablas

Tabla 1 Documentación y requisitos de garantía de seguridad _____18

Tabla 2 Justificación de cobertura de dependencias _____19

Índice de figuras

<i>Ilustración 1: Arquitectura lógica del TOE</i>	<u>12</u>
<i>Ilustración 2: Entorno operacional del TOE</i>	<u>12</u>
<i>Ilustración 3: Modelo de base de datos del registro de información</i>	<u>20</u>

Acrónimos

CC	Common Criteria
DGTrans	Dirección General de Transportes Terrestres
EAL	Evaluation Assurance Level
FNMT-RCM	Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda
J2EE	Plataforma Java Edición Enterprise
PPT	Pliego de prescripciones técnicas
TC	Tarjeta del conductor
TOE	Objetivo de la Evaluación (Target Of Evaluation)
TSF	TOE Security Functionality
VU	Unidad Vehicular (tacógrafo)
BBDD	Base de datos
PK_{EU}	Clave pública europea
HTTP	Hipertexto Transfer Protocolo
SOAP	Simple Object Access Protocol

Relación de documentación

Documento	Versión
Anexo 1B del Reglamento CE 1390/2002	5.8.2002

Control de versiones

Versión del documento: **1.6**

Histórico de versiones:

Versión	Fecha	Observaciones
1.0	02/10/2008	Primera versión del documento
1.1	21/10/2008	Actualización de la descripción y corrección de los SFR
1.2	23/10/2008	Adicción del requisito FDP_DAU.1 con la representación gráfica
1.3	15/01/2009	Modificación del resumen alineándolo con la descripción y corrección de los objetivos de seguridad para el entorno con respecto a la PDA
1.4	15/01/2009	Modificación de la operación de selección del canal seguro, únicamente el TOE inicia el canal seguro. Y en la especificación funcional el FTP_ITC.1 aplica a la exportación de datos
1.5	11/05/2009	Adaptación de la declaración de seguridad a los cambios inducidos de por el análisis de vulnerabilidades.
1.6	11/06/2009	Nueva versión del producto a 5.0 y corrección de errores tipográficos

1 Identificación de la Declaración de Seguridad

DOCUMENTO:	DECLARACIÓN DE SEGURIDAD. DESCARGA DE DATOS DEL TACÓGRAFO DIGITAL
AUTOR:	FNMT-RCM
REVISADO	FNMT-RCM
VERSIÓN:	1.6
FECHA:	12/05/2009

1.1 Identificación del Objetivo de la Evaluación

Fabricante: FNMT-RCM

Nombre del producto: Aplicación de descarga de datos del tacógrafo digital

Versión: 5.0

1.2 Resumen

Esta declaración de seguridad establece las bases para la evaluación de seguridad según normativa Common Criteria v3.1 rev. 2 y CEM v3.1 rev. 2, con conformidad EAL1 de un producto tipo aplicación software.

El Objetivo de la Evaluación (TOE) es la aplicación de Análisis y descarga de datos procedentes del Sistema del Tacógrafo Digital.

El TOE es un programa informático (desarrollado en tecnología J2EE) que se ejecuta en un servidor de aplicaciones (Oracle IAS 10.1.3) que controla la información procedente de las descargas (mediante la ejecución remota métodos en plataformas clientes con soporte J2ME o J2SE) de las tarjetas de conductores y de los propios tacógrafos digitales (con que se equipan los vehículos que realizan el transporte por carretera) mediante firma digital, para su posterior almacenamiento en una base de datos (Oracle 9i).

1.3 Ajuste a la norma “Common Criteria”

Pliego de prescripciones técnicas para el desarrollo del “**Centro de Análisis y Descarga de Datos**” dentro del proyecto de **Desarrollo e implantación del sistema de control de transportes por carretera** del Ministerio de Fomento.

Esta declaración de seguridad cumple con los requisitos de la norma CC v. 3.1 Parte 1 revisión 1, CC v 3.1 Parte 2 revisión 2 y CC v. 3.1 Parte 3 revisión 2 y define conformidad con el paquete EAL1.

Debido a que no se definen requisitos extendidos de seguridad funcional o de garantía, cumple conformidad estricta con la norma CC parte 2 y 3

La selección del nivel de conformidad, EAL1, se justifica por la necesidad de garantía de las propiedades de seguridad del producto, que vienen dictadas por el PPT (Pliego de Prescripciones Técnicas).

2 Descripción del producto a evaluar.

La funcionalidad del TOE es controlar y gestionar el flujo de información utilizando firmas digitales para la verificación de los bloques de datos en el proceso de descarga de los bloques de datos procedentes del tacógrafo digital y posteriormente almacenarlos de forma segura incluyendo las firmas digitales en una base de datos confiable.

El TOE es un programa informático (desarrollado en tecnología J2EE) que se ejecuta en un servidor de aplicaciones (Oracle IAS 10.1.3). Este servicio mediante tecnología Java RMI y HTTP – SOAP publica métodos remotos, que son ejecutados en las plataformas PDA con soporte J2ME que llevan los agentes o inspectores del Cuerpo Nacional de Policía.

La ejecución de este método remoto permite:

- Importar la información de datos de las tarjetas de conductores y de los propios tacógrafos digitales, verificando la integridad de los bloques de datos mediante la firma digital, (y su posterior procesado para generar infracciones en base a controles establecidos en Anexo 1B del REGLAMENTO (CE) No 1360/2002)¹. Exportar a una base de datos (Oracle 9i), dejando evidencia de validez e integridad de los datos procesados.

Los bloques de datos que conforman los ficheros de datos (extraídos de la VU y TC) se transformarán en estructuras de datos (clases Java), siguiendo lo especificado en el Anexo 1B del REGLAMENTO (CE) No 1360/2002.

El TOE permite la importación de claves públicas o certificados que son usadas para validar las firmas digitales y que es conforme con lo que establece el Anexo 1B del REGLAMENTO (CE) No 1360/2002

¹ La funcionalidad de procesado queda fuera del alcance de aplicación del TOE

El esquema lógico del TOE es:

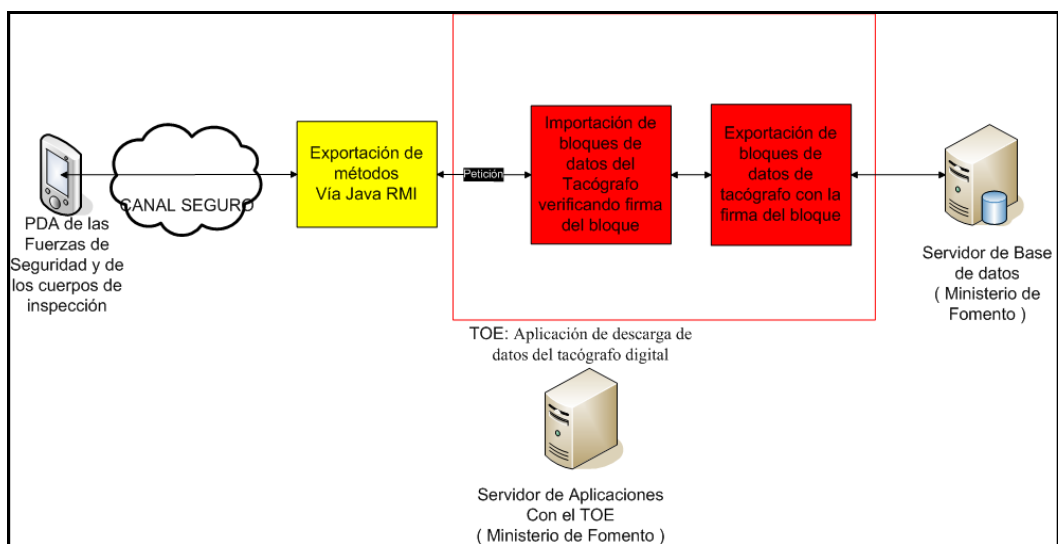


Ilustración 1: Arquitectura lógica del TOE

El esquema físico del TOE en su entorno de aplicación es:

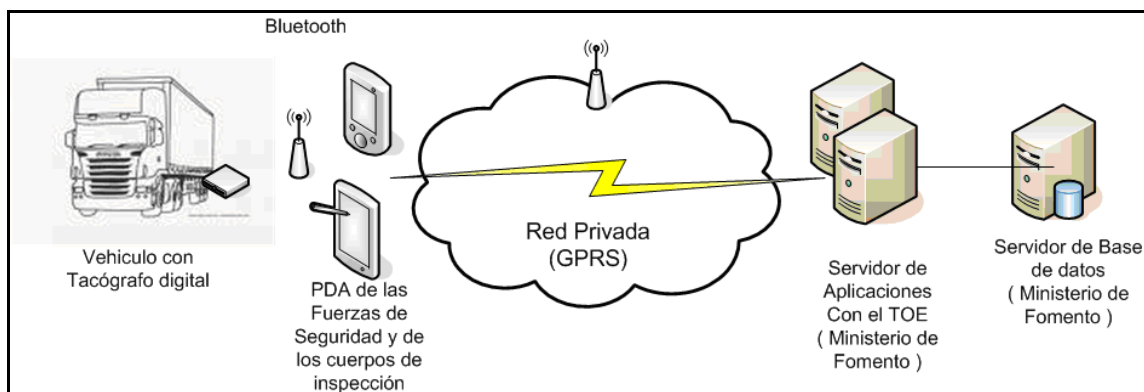


Ilustración 2: Entorno operativo del TOE

3 Objetivos de seguridad para el entorno

3.1 Objetivos del entorno IT

El servidor de aplicaciones dónde se ejecuta el TOE está situado en una ubicación segura y controlada por medio de administradores confiables pertenecientes a la Administración del Estado.

El servidor de base de datos dónde se guardan los datos es confiable y está situado en una ubicación segura y controlada por medio de administradores confiables pertenecientes a la Administración del Estado.

El acceso al TOE por medio de las PDA, (confiables y conformes con la extracción de datos del tacógrafo especificada en el Anexo 1B del REGLAMENTO (CE) N° 1360/2002), de los agentes o inspectores para la ejecución de métodos remotos se realizará mediante un canal seguro de comunicaciones que asegurarán la autenticidad e integridad de los datos transmitidos.

4 Requisitos de seguridad.

4.1 Requisitos funcionales de seguridad

4.1.1 FDP_ETC.2 Export of user data with security attributes

Hierarchical to: No other components.

Dependencies: [FDP_IFC.1 Subset information flow control
or FDP_ACC.1 Subset access control]

FDP_ETC.2.1 The TSF shall enforce the [assignment: *política de flujo de datos*] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE: [assignment: *verificación de la firma digital de los bloques de datos*].

4.1.2 FDP_ITC.2 Import of user data with security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control
or FDP_IFC.1 Subset information flow control]

[FTP_ITC.1 Inter-TSF trusted channel
or FTP_TRP.1 Trusted path]

FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_ITC.2.1 The TSF shall enforce the [assignment: *política de flujo de datos*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *verificación de la firma digital de los bloques de datos*].

4.1.3 FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [assignment: *política de flujo de datos*] on [assignment: *operación de importación/exportación de datos procedentes del tacógrafo digital*].

4.1.4 FPT_TDC.1 Inter-TSF basic TSF data consistency

Hierarchical to: No other components.

Dependencies: No other components.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [assignment: *la firma digital de los bloques de datos de tacógrafo*] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [assignment: *especificación descrita en el Anexo 1B del REGLAMENTO (CE) No 1360/2002*] when interpreting the TSF data from another trusted IT product.

4.1.5 FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [assignment: *política de flujo de datos*] based on the following types of subject and information security attributes: [assignment: *bloque de datos obtenidos de TC y VU mediante atributos de seguridad de firma digital de los bloques de datos) y Certificados mediante atributos de seguridad: firma digital del certificado*].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment:

- *Operación verificación de firma: que la firma digital de los bloques de datos sea correcta.*
- *Operación verificación de certificado: que todas las firmas digitales implicadas en la operación de verificación del certificado (verificación de la cadena de certificados) sean válidas.*

].

FDP_IFF.1.3 The TSF shall enforce the [assignment: *ninguna*].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *ninguna*]

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment: *ninguna*].

4.2 Requisitos de garantía de seguridad

Los requisitos de garantía de seguridad para el TOE son los definidos en el paquete EAL1 especificados en CC versión 3.1 Release 2

4.3 Justificación de requisitos de seguridad

Los requisitos de garantía de seguridad se justifican mediante la presentación a la evaluación de los distintos documentos que acreditan el cumplimiento de los correspondientes requisitos.

Componente	Evidencia
ADV_FSP.1: Basic Functional specification	Declaración de seguridad: Descarga de datos procedentes del Tacógrafo Digital versión 1.6 Especificación Funcional, Versión 1.3 Manual de Usuario, Versión 1.0
AGD_OPE.1: Operational User Guidance	Declaración de seguridad: Descarga de datos procedentes del Tacógrafo Digital versión 1.6 Manual de Usuario, Versión 1.0 Especificación Funcional, Versión 1.3
AGD_PRE.1: Preparative Procedures	Declaración de seguridad: Descarga de datos procedentes del Tacógrafo Digital versión 1.6 Manual de Usuario, Versión 1.0 TOE
ALC_CMC.1: Labelling of the TOE	Declaración de seguridad: Descarga de datos procedentes del Tacógrafo Digital versión 1.6 TOE
ALC_CMS.1: TOE CM Coverage	Declaración de seguridad: Descarga de datos procedentes del Tacógrafo Digital versión 1.6 Listado de datos de configuración, Versión 1.0
ASE_CCL.1: Conformance claims	Declaración de seguridad: Descarga de datos procedentes del Tacógrafo Digital versión 1.6
ASE_ECD.1: Extended components definition	Declaración de seguridad: Descarga de datos procedentes del Tacógrafo Digital versión 1.6
ASE_INT.1: ST introduction	Declaración de seguridad: Descarga de datos procedentes del Tacógrafo Digital versión 1.6

ASE_OBJ.1: Security objectives	Declaración de seguridad: Descarga de datos procedentes del Tacógrafo Digital versión 1.6
ASE_REQ.1: Stated Security Requirements	Declaración de seguridad: Descarga de datos procedentes del Tacógrafo Digital versión 1.6
ASE_TSS.1: TOE summary specification	Declaración de seguridad: Descarga de datos procedentes del Tacógrafo Digital versión 1.6
ATE_IND.1: Independent testing - conformance	Declaración de seguridad: Descarga de datos procedentes del Tacógrafo Digital versión 1.6 Especificación Funcional, Versión 1.3 Manual de Usuario, Versión 1.0 TOE
AVA_VAN.1: Vulnerability survey	Declaración de seguridad: Descarga de datos procedentes del Tacógrafo Digital versión 1.6 Manual de Usuario, Versión 1.0 TOE

Tabla 1 Documentación y requisitos de garantía de seguridad

Los requisitos funcionales de seguridad se justifican mediante la inclusión de los requisitos funcionales con dependencias o con una justificación.

SFR	Dependencia	Justificación
FDP_ETC.2	<ul style="list-style-type: none"> [FDP_IFC.1 or FDP_ACC.1] 	Se ha incluido el componente FDP_IFC.1
FDP_ITC.2	<ul style="list-style-type: none"> [FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1] FPT_TDC.1 	Se han incluido los componentes FDP_IFC.1 y FPT_TDC.1. No se ha incluido la dependencia [FTP_ITC.1 ni FTP_TRP.1] ya que es el entorno el que proporciona el canal seguro entre las PDA de los agentes o inspectores y el TOE
FDP_IFF.1	<ul style="list-style-type: none"> FDP_IFC.1 FMT_MSA.3 	Se ha incluido el componente FDP_IFC.1. No se ha incluido FMT_MSA.3, ya que la importación de los bloques de datos del fichero de datos (TC o VU) se hace mediante la verificación de una firma digital y por tanto no hay atributos de seguridad estáticos

Tabla 2 Justificación de cobertura de dependencias

5 Resumen de la especificación

Las funcionalidades de seguridad que proporciona el TOE son:

1. **Exportación de datos resultantes**, Los bloques de datos que conforman los ficheros de datos obtenidos de TC y VU se transformarán en estructuras de datos (clases Java) siguiendo lo especificado en el Anexo 1B del REGLAMENTO (CE) No 1360/2002.

El registro de la información se realiza incluyéndola en tablas de una base de datos. Las tablas que intervienen en dicho proceso son las siguientes:

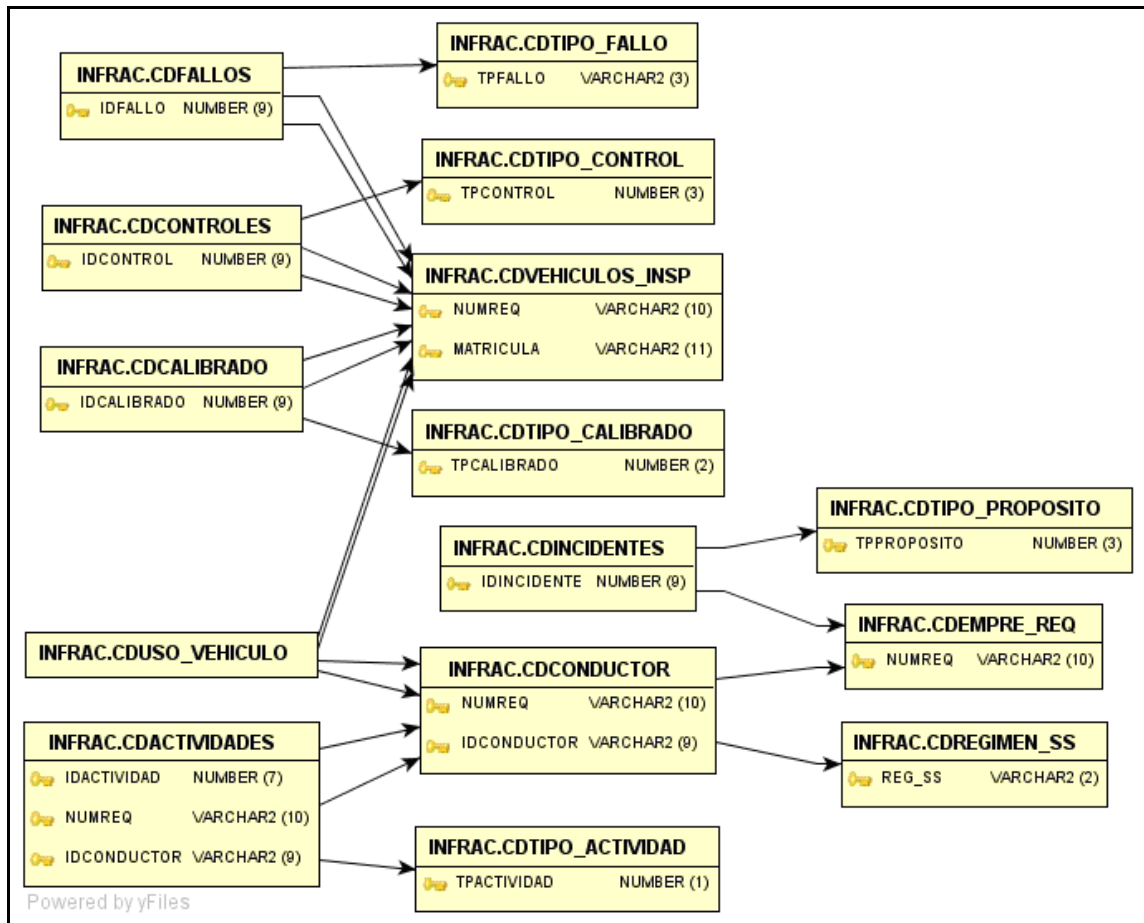


Ilustración 3: Modelo de base de datos del registro de información

Justificación de cobertura de SFR:

- a. FDP_ETC.2, FDP_IFC.1 y FDP_IFT.1 se cubren mediante el volcado de los datos resultantes en las clases genéricas enlazadas con la BBDD y el almacenado de los datos completo incluyendo la firma digital
2. **Importación de fichero de datos**, el volcado de los bloques de datos de los Ficheros a datos extraídos de la tarjeta TC y de la VU vienen firmados digitalmente, las comprobaciones de seguridad que se realizan para este tipo de fichero son:
- Extracción de la clave pública del tacógrafo. Utilizando la clave pública de primer nivel (nivel europeo) PK_{EU} se comprobará la integridad del registro “resumen” en el que se encuentran los certificados del estado miembro y del equipo.
 - Comprobación de integridad de cada bloque de datos. Con la clave pública del equipo se verificará la integridad de cada uno de los bloques de datos del fichero antes de proceder a la importación en las estructuras de datos (clases Java) siguiendo lo especificado en el Anexo 1B del REGLAMENTO (CE) No 1360/2002.

Justificación de cobertura de SFR:

- a. FDP_ITC.2, FDP_IFC.1, FDP_IFT.1, se cubre mediante la importación de los bloques de datos del fichero de datos TC o VU comprobando la firma digital de éstos
- b. FPT_TDC.1, se cubre al recibir los bloques de datos del fichero de datos, la aplicación es capaz de procesar la información e identificar los campos que lo componen y poderlos relacionar posteriormente con la Firma del bloque de datos del fichero de TC o VU